UNITED STATES PATENT AND TRADEMARK OFFICE

MN

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/844,448	04/27/2001	Gregory Neil Houston	05456.105005	9082

69151 7590 05/09/2007
KING & SPALDING, LLP
INTELLECTUAL PROPERTY DEPT. - PATENTS
1180 PEACHTREE STREET, N.E.
ATLANTA, GA 30309-3521

EXAMINER	
PICH, PONNOREAY	
ART UNIT	**PAPER NUMBER**
2135	
MAIL DATE	**DELIVERY MODE**
05/09/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 09/844,448
Filing Date: April 27, 2001
Appellant(s): HOUSTON ET AL.

Kelly L. Broome (Reg. # 54,004)
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 2/20/2007 appealing from the Office action mailed 11/17/2006.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

6,088,804	Hill et al	6-2000
6,775,657	Baker	8-2004

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claims 27-29 and 31-32 are rejected under 35 USC 102(e) as being anticipated by Hill et al (US 6,088,804).

Claims 1-26 and 33-59 are rejected under 35 USC 103(a) as being unpatentable over Hill et al (US 6,088,804) in view of Baker (US 6,775,657).

These rejections are set forth in the Final Office action mailed on 11/17/2006.

(10) Response to Argument

Please note that to make it easier for the reader to follow along, the examiner will use the same headings as the appellant in traversing appellant's arguments.

Rejection of claims as obvious over 35 USC 102(e)

First the examiner notes that with respect to appellant's heading that the question of obviousness falls under 35 USC 103, while anticipation falls under 35 USC 102. Thus the examiner assumes the above heading used by appellant which refers to rejection of claims as "obvious" over 35 USC 102(e) as being an unintentional mistake.

Independent Claim 27

Appellant's arguments with respect to claim 27 begin on page 13 of appeal brief filed and continue to page 17. Appellant argues that Hill does not teach "an event manager that is operable for analyzing and filtering the security event data with scope criteria comprising one or more defined variables operable for analyzing and filtering the security event data" (see page 16 of appeal brief). Appellant argues that simply displaying attack status information as taught by Hill is not the same as "analyzing and filtering the security event data with scope criteria comprising one or more defined variables operable for analyzing and filtering the security event data". The examiner respectfully disagrees. Even appellant's summary of what Hill teaches (pages 13-16 of filed appeal brief) shows that this limitation is met by Hill. On page 14 of the appeal brief, appellant states that Hill discloses a database of simulated attack information. The simulated attack information/attack signatures can be considered "scope criteria comprising one or more defined variables operable for analyzing and filtering security event data" since it is used for comparison with network event data to determine if the event data corresponds to any known attack types as well as used to determine the severity of the attack. Note that as discussed in cited column 5, lines 46-50, the signature of the attacks are defined by at least one security event, i.e. defined variables. In the first two paragraphs on page 16 of the filed appeal brief, appellant summarizes how Hill's system monitors and analyzes network traffic data, i.e. security event data, comparing the network traffic data to the simulated attack signatures stored in a database as seen in Figure 3 of Hill. This analysis is then used to form the network display seen in Figure 7 of Hill. Display map 66 in Figure 7 shows the attacks, i.e. security event data, having been sorted/filtered by severity (col 6, lines 53-60 of Hill) and by attack type (col 6, lines 61-67 of Hill). Despite appellant's argument that simply displaying attack status information is not the same as "analyzing and filtering the security event data with scope criteria comprising one or more defined variables operable for analyzing and filtering the security event data", the examiner respectfully submits that unless the network event data, i.e. security event data, were analyzed and filtered using the attack signatures, i.e. scope criteria, stored in database 48, the attacks could not have been filtered by attack severity and attack type for display. The data is also analyzed and filtered so that the security event type and location is also determined as evidenced by table 108 in Figure 7.

In short, analyzing and filtering the security event data with scope criteria which comprises one or more defined variables...reads on Hill's teachings of comparing the network traffic data with the signature data stored in the database and displaying the result of the analysis based on attack severity and type as seen in Figure 7. If analysis and filtering of the network traffic data was not done, then Hill's invention could not have displayed the attacks by severity, type, and location. The component of Hill's invention that performed these processes can be considered an event manager.

Dependent Claims 28-33

Appellant's arguments for claims 28-33 are based on dependency on claim 27 and are traversed because the arguments for claim 7 are traversed.

Rejection of claims as obvious over 35 USC 103(a)

Independent claims 1, 16, 34, and 49

In the paragraph which spans pages 18-19 of the filed appeal brief, appellant argues that Hill and Baker fails to teach: (1) providing one or more variables operable for analyzing and filtering the security event data, the variables comprising at least one of a location of a security event, a source of security even, a destination of the security event, a security event type, a priority of a security event, and an identification of a system that detected a security event"; (2) "creating scope criteria by selecting one or more of the variables operable for analyzing and filtering the security event data"; and (3) "analyzing and filtering the collected security event data with the scope criteria to produce result data". The examiner respectfully disagrees—Hill does in fact teach all three of these limitations.

As per the limitation of providing one or more variables operable for analyzing and filtering the security event data, the variables comprising at least one of a location of a security event, a source of security event, a destination of the security event, a security event type, a priority of a security event, and an identification of a system that detected a security event, it is met by Hill having the database of simulated attacks, i.e. attack signatures (col 5, lines 21-37). The cited section shows that the simulated attack is a defined by a plurality of security events, i.e. variables. Those variables comprise at least the location of a security event, source of a security event, and a security event type (col 5, line 45-col 6, line 8). As discussed in the traversal of claim 27, the variables which makes up the attack signatures are used, i.e. operable, for analyzing and filtering the security event data. Thus the limitation is met by Hill.

As per the limitation of creating scope criteria by selecting one or more of the variables operable for analyzing and filtering the security event data, the sections cited in the Final Office action (col 5, line 46-col 6, line 5) shows that the training signatures/attack signatures for simulated attacks are comprised of security event types, i.e. variables, which includes at least the location of a security event, source of a security event, and a security event type. These variables are operable for analyzing and filtering the security event data. The claimed scope criteria read on the disclosed training signatures formed from one or more selected security event types and because they exist in Hill's invention, they were created. Thus, the limitation is met by Hill.

As per the limitation of analyzing and filtering the collected security event data with the scope criteria to produce result data, it was already discussed in the traversal of claim 27 how Hill taught analyzing and filtering the collected security event data with the scope criteria. The result of the analysis and filtering is the output display seen in Figure 7, i.e. result data that is produced.

It is noted that while appellant argues that the references do not teach the above limitations under contention, appellant did not argue whether or not the references are combinable to reject the claims as a whole under 35 USC 103. Appellant also did not argue the motivation given in the Final Office action for combining the two references. As such, it is assumed that appellant agrees that the references are combinable and that one of ordinary skill in the art of networking and network security would have been motivated to combine the teachings of Hill and Baker for the reason given in the Final Office action in the third paragraph on page 10, i.e. for availability purposes. Thus claims 1, 16, 34, and 49 were properly rejected under 35 USC 103 as being obvious over Hill and Baker since the combination of Hill and Baker renders obvious all the limitations recited in the claims and it was established that one of ordinary skill in the art would have been motivated to combine the teachings of the prior art as recited in the claims.

Dependent Claims 2-15, 17-26, 35-48, and 50-59

The arguments for these claims are based on dependency on claims 1, 16, 34, and 49. Because the independent claims are not allowable, the dependent claims are also not allowable.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

Ponnoreay Pich

Ponnoreay Pich

Conferees:

Gilberto Barron Jr. (SPE)

Benjamin Lanier

GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100